REMARKS

The Examiner is thanked for the performance of a thorough search. By this amendment, Claims 1-5, 9, 13, 14, 16-18 have been amended and claim 12 has been cancelled. Accordingly, Claims 1-11 and 13-22 are pending in this application. The amendments to the claims do not add any new matter to this application. Furthermore, the amendments to the claims were made to improve the readability and clarity of the claims and not for any reason related to patentability. Each pending claim is in condition for allowance over the cited art because one or more elements of each pending claim is not disclosed, taught, or suggested by the cited art.

REJECTION OF CLAIMS 9 AND 14 UNDER 35 U.S.C. § 112

Claims 9 and 14 stand rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regard as the invention. In particular, the Office Action noted that claims 9 and 14 recite the limitation "request to from". The Examiner is correct in the assumption that the limitation is meant to read "request from." Claims 9 and 14 have been amended in this paper remove the noted typographical error.

Applicants therefore respectfully request withdrawal of the rejection under 35 U.S.C. § 112, second paragraph.

REJECTION OF CLAIMS 1-22 UNDER 35 U.S.C. § 103(a)

Claims 1-4 and 9-18 were rejected under 35 U.S.C. § 102(e) as being unpatentable over *An*, U.S. Patent No. 6,031,904. Claims 5-8 and 19-22 were rejected under 35 U.S.C. §

102(e) as being unpatentable over *An* in view of *Sladek*, U.S. Patent No. 6,622,016. The rejections are herein respectfully traversed.

The claimed invention is fundamentally different than the systems disclosed in *An* and *Sladek*. *An* teaches a system for allowing users to update telephone feature profiles for a specified Directory Number (DN) over the Internet. *An* teaches validating the user's right to modify services for the specified DN through the use of a password or PIN. (Col. 5, lns 12-13; Col. 7, lns 50-55). Upon validation, the *An* system provides the user with the ability to view and update features for the specified Directory Number. (Col. 5, lns 18-48).

The system in *An* allows a user to log in using a single DN and PIN, and modify that DN's feature profile. If the user happens to have multiple Directory Numbers, for example a cell phone number and landline number, he will have to separately log in using the DN for the second line if he wants to modify the feature profile for a second line. The feature profiles are associated with DN, not with the subscriber user. Furthermore, a user may change any feature in the feature profile of the DN once his DN and PIN have been validated.

The claimed invention is completely different is several aspects. First, when a user logs in a system of the claimed invention, he can view and modify his subscription to one *or more* telecommunications *services* through the same session. For example, a subscriber can subscribe to such multiple services as teleconferencing, streaming video, personalized Internet, business grade Internet, shopping and gaming, and can modify which services that he is subscribed to through a single session in the claimed invention. (See Page 2, line 1). The claims all require that a subscriber to subscribe to *one or more* telecommunications

services. The telephone feature profile of *An* does not read on subscribing to one or more telecommunication services.

An only allows a user to update the feature profile of a single DN. (Col. 2, lines 1-10). If the user wants to modify the feature profile for a different line, he will have to log in using the DN and PIN for that line. The feature profiles are associated with DN, not with the subscriber user. The Office Action asserts in Section 2 that upon positive verification "the subscriber is presented with all the features/services they currently subscribe to." However, because a user in *An* can only log in using one DN, it is not possible for a subscriber to be presented with all the features/services they currently subscribe to, because, as the Office Action notes, "a subscriber in *An* may have more than one line, i.e. a landline, a wireless subscription, pager service, local and/or long distance service..." (Office Action, Page 4, last paragraph). A user cannot log in and have access to all of the feature profiles of all of his lines or services. Only the feature profile for a single DN is accessed.

Second, if two people use one particular line and have access to the PIN, either person can log in to the *An* system and modify the feature profile for that DN. Each line in *An* has its own DN, and each DN has a separate feature profile (Col. 2, lns 1-3). Authentication is separate for each line or DN. The authentication process is *An* is DN-specific, not user-specific.

In contrast, the services in the claimed invention are associated with a subscriber, not with a DN. Claim 1 requires "modifying a subscription of a subscriber to one or more services based on subscriber information and service information." Claim 9 requires a method of "automatically logging in a subscriber to all telecommunications services

-20-

subscribed to by the subscriber <u>based on subscriber information and service information</u>." *An*

does not teach any type of subscriber information. Authentication is through a DN and PIN

only.

Third, the claimed invention uses the subscriber information to provide for

differentiated services, whereby each user may have a different level of authority to make

modifications to his subscription. As is described in the Background section of the present

application, prior art service subscription management systems suffer from the lack of a

separate authorization model. (Page 2, lns 16-17). As in *An*, any user can subscribe to any

service. In order to provide differentiated services, an authorization model is essential. The

claimed invention allows for differentiated service levels through a user privilege token.

The claimed invention uses information about the user, such as his role within an

organization, to determine his access rights, which may be different than another user. As

discussed above, *An* is DN-specific, not user-specific. Once a user logs into the system of *An*

with a DN, he can update anything in the feature profile for that DN. Two people can log

into the *An* system and update the feature profile for a DN.

The claimed invention uses a privilege token associated with a subscriber or privilege

information associated with a subscriber to provide differentiated authority to modify

subscriptions.

As is required by independent claims 1 and 16-19, the claimed invention requires:

determining, based on privilege information in a privilege token associated with the
subscriber generated by the authorization service, whether the subscriber has
privileges sufficient to carry out the requested modification.

Likewise claim 5 requires:

determining, based on privilege information in a privilege token that is associated with the administrator and is generated by an authorization service, whether the administrator has privileges sufficient to carry out the request modification.

Claim 13 requires:

privilege information associated with the subscriber specifying what telecommunications services the subscriber has privileges to subscribe to.

The Office Action states at Page 4, first paragraph, that a token is known and that it would have been obvious to use a privilege token method of validation. However, the claimed invention requires authorization through a privilege token associated with the subscriber (Claims 1, 16-18). Alternatively, the privilege token is associated with the administrator (Claim 13); or privilege information is associated with the subscriber (Claim 13); or authorization information is associated with the subscriber (Claims 19-22).

An only teaches that a DN and PIN are validated, and does not disclose or suggest any differentiated authorization levels. *An* does not teach or suggest privilege tokens, or even privilege information associated with a subscriber.

A subscriber's role within an organization may be used by the claimed invention determine his access rights. Independent claims 19-22 and dependent claims 2 and 14 all require a "role occupied by a subscriber" or a "role of the subscriber" wherein access permissions are associated with the subscriber's role.

The Office Action asserts at Page 4, last paragraph, that "more than one line, i.e. a landline, a wireless subscription, page service, local and/or long distance service, etc. read as the claimed roles." However, as the present specification teaches at Page 8, line 11 through Page 9, line 5, a "Role" is personal to the subscriber user. In particular, the specification states that "improved authorization processing is achieved using role-based access control.

Access permissions are associated with Roles, and users are made members of Roles. In one embodiment, role-based access control allows the definition of security policies that closely match enterprise operations."

The different lines of *An* are inapplicable to the "role" as required by the presently claimed invention. Multiple telephone lines cannot read on Roles as required in the claims invention. Furthermore, it is not possible to modify *An* such that the user's role in an organization can be used to determine which features in a feature profile that the user can modify, as *An* does not use any subscriber information, only DN information.

Fourth, the claimed invention requires that a subscriber user is authenticated by an authentication server, and that privileges to modify subscriptions are determined by a privilege token generated for the user by an authorization service. The authentication server 106 is completely separate from the authorization service 114, as shown by Fig. 1.

As described in the current specification at Page 4, lines 22-25, "service management and selection is separated from user authentication processing. As a result, any of a plurality of authentication methods may be used in the system without altering the user or service management." Because authorization is a separate aspect of the present invention, "a user may modify only those attributes for which the user has been granted rights to modify." (Page 7, line 25 – Page 8, line 1). "Authentication is considered separate from user and account management. Improved authorization processing is achieved using role-based access control." (Page 8, lines 11-12).

An only teaches validating a DN and PIN. There is no separate authorization process or service taught or suggested anywhere in *An*.

Independent claims 1 and 16-18 require both an authentication server and an authorization service. Independent claim 9 requires separate steps for authenticating a subscriber by an authentication server and generating a privilege token by an authorization service.

Fifth, claim 9 is directed to automatically logging a subscriber to all telecommunications services subscribed to by the subscriber. After an authentication process and a separate authorization process, the subscriber has access not only to update subscriptions, but also has access to the subscribed services. For example, if the subscriber subscribes to videoconferencing and business grade Internet services, he has access to both through a single login. (The auto-login process is described at Page 17 line 20 – Page 19, line 9). The subscriber in the claimed invention has actual access to the *services*, not just a feature profile for a DN

With respect to Claim 9, the Office Action states that *An* teaches that "besides merely displaying a subscriber's current feature profile to them, the subscriber is actually "logged in" as they are able to amend each feature on their current profile." (Page 5, second paragraph). However, it is not possible to log into the actual phone service in the system of *An*. *An* only provides for accessing a feature profile of a DN, not the service of the DN itself. *An* only teaches "access to that subscriber's telephone feature profile for viewing and optionally changing, adding or deleting features by the subscriber." (Col. 2, lns 8-10). It is not possible for a user to log in to any service in *An*, much less automatically be logged into all subscribed telecommunication services.

Finally, with respect to Claim 5, the Office Action states that *Sladek* could be combined with *An* to teach modifying subscriptions of a group of subscribers. In particular, the Office Action states at Page 6, last paragraph, that "instead of providing service to one subscriber, it would be to a group of subscribers, linked in some manner in the profile repository." As discussed above, authentication and the profile repository are associated with a specific DN. It is not possible that profile repositories of multiple DNs can be accessed in *An.*. In addition, as discussed above, authentication is associated with a DN, not a subscriber, so it is not possible to form a group of subscribers in *An*, even if it were possible to form a group of DNs.

Applicants respectfully request withdrawal of the rejection under 35 U.S.C. 103(a) for independent claims 1, 5, 9, 13 and 16-22. Dependent claims 2-4, 6-8, 10-11 and 14-15 all include the limitations of the independent claims by virtue of their dependence. It is therefore respectfully submitted that the dependent claims are patentable over the cited art for at least the reasons set forth herein with respect to the independent claims.

Furthermore, it is respectfully submitted that the dependent claims recite additional limitations that independently render them patentable over the cited art.

For example, the Office Action asserts that the limitations of Claims 3, 4, 7 and 8 merely address the programming level aspect of the invention, and that use of object-oriented programming languages or protocols are inherent. However, claim 3 specifically requires not just an object, but a "host object" that uniquely identifies the subscriber and contains a privilege token corresponding to the subscriber. The required Host Object is more than just an object-oriented programming construct, and is not inherent. The Host Object of the

claimed invention, as required by claim 3, uniquely identifies the authenticated subscriber

and is used to store the privileges token generated by the authorization service.

Claim 11 requires that the privilege token generated by the authorization service is

stored in a service selection gateway for subsequent authorization processes relating to the

subscriber. With respect to Claim 11, the Office Action states on Page 5, last full paragraph,

that *An* teaches the use of a subscriber service provisioning manager, and that it reads as the

claimed selection gateway. The Office Action fails to state how a privilege token generated

by an authorization service (not authentication, as noted above), is stored in a service

selection gateway for subsequent authorization processes relating to the subscriber as

required by Claim 11. *An* fails to teach any subsequent processing of a user after the initial

DN validation, or any kind of privilege token generated by an authorization service.

Conclusion

It is respectfully submitted that all of the pending claims are in condition for

allowance and the issuance of a notice of allowance is respectfully requested. If there are

any additional charges, please charge them to Deposit Account No. 50-1302.

The Examiner is invited to contact the undersigned by telephone if the Examiner

believes that such contact would be helpful in furthering the prosecution of this application.

©

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

Lesley Coulson Boveri

Lesley Coulson Boveri
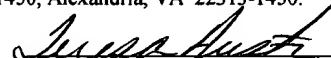Reg. No. 46,642
Date: July 6, 2004

1600 Willow Street
San Jose, CA 95125
(408) 414-1210
Facsimile: (408) 414-1076